

Uncoordinated Frequency Shifts based Pilot Contamination Attack Detection

Weile Zhang and Hai Lin[†]

MOE Key Lab for Intelligent Networks and Network Security, Xi'an Jiaotong University, Xi'an, China

[†]Department of Electrical and Information Systems, Osaka Prefecture University, Osaka, Japan

wlzhang@mail.xjtu.edu.cn, lin@eis.osakafu-u.ac.jp

Abstract—Pilot contamination attack is an important kind of active eavesdropping activity conducted by a malicious user during channel training phase. In this paper, motivated by the fact that frequency asynchronism could introduce divergence of the transmitted pilot signals between intended user and attacker, we propose a new uncoordinated frequency shift (UFS) scheme for detection of pilot contamination attack in multiple antenna system. An attack detection algorithm is further developed based on source enumeration method. Both the asymptotic detection performance analysis and numerical results are provided to verify the proposed studies. The results demonstrate that the proposed UFS scheme can achieve comparable detection performance as the existing superimposed random sequence based scheme, without sacrifice of legitimate channel estimation performance.

Index Terms—Physical layer security, pilot contamination attack, uncoordinated frequency shift (UFS).

I. INTRODUCTION

As an effective way to protect wireless transmissions from being eavesdropped, physical layer security has been drawing substantial research interests. Recent results in physical layer security methods require full or partial knowledge about channel state information of the legitimate system, which is quite vulnerable to smart malicious attacks. A typical example in a TDD system is the so-called pilot contamination attack from an active eavesdropper [1]. As illustrated in Fig. 1, the eavesdropper (Eve) wants to overhear the communication from the legitimate transmitter (Alice) to the intended receiver (Bob). During the reverse uplink training phase, Bob sends training (pilot) signal to Alice, and the latter performs legitimate channel estimation based on channel reciprocity. Unfortunately, during the training phase, the active eavesdropper Eve can also send the same pilot signals, thereby biasing the channel estimation at Alice. This not only degrades the signal reception quality at Bob but also leads to a significant signal leakage to Eve during the subsequent downlink data transmission.

The issue of above pilot contamination was first noted in [1] and a few works have been further reported to detect such smart attacks. For example, the random pilot sequence was employed in [2] to detect the presence of attack. A few number of detection schemes were studied in [3] assuming different knowledge about the large-scale fading parameters. A two-way training scheme for discriminatory channel estimation was proposed in [4] though a whitening-rotation based semiblind method. Based on the Neyman-Pearson criterion, a number of detection methods were developed in [5] under different

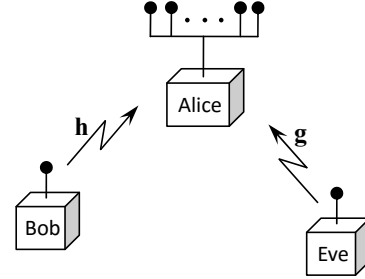


Fig. 1. Alice is a multi-antenna base station sending messages to the intended user Bob, while Eve is a malicious single-antenna eavesdropper.

assumptions about the channel and noise statistics. The authors in [6] proposed an energy ratio detector, by exploring the asymmetry of received signal power levels at the transmitter Alice and legitimate receiver Bob in the presence of an attack. Another recent work in [7] proposed superimposing a random sequence on the training sequence at the Bob, allowing use of source enumeration methods to detect attack. The idea was further extended to the multiuser TDD/SDMA uplink scenario [8].

All of the above detection works have assumed perfect frequency synchronization in the system. However, carrier frequency offset (CFO) naturally exists due to frequency mismatch between transceiver oscillators [10], [11]. This means both the legitimate user Bob and the attacker Eve should first perform CFO estimation and oscillator frequency calibration, such that the carrier frequency of their training signals can be aligned to Alice. Although the CFOs are expected to be completely eliminated for data transmission, however, they may be beneficial to the purpose of pilot contamination attack. Note that even the same pilot signals are transmitted from Bob and Eve, the natural CFOs would bring in individual phase shifts and thus result in divergence of the transmitted signals.

Motivated by the above observation, we propose a new uncoordinated frequency shift (UFS) scheme for detection of pilot contamination attack in multiple antenna system. During the reverse training phase of the UFS scheme, Bob deliberately introduces multiple random frequency shifts when transmitting the publicly known pilot sequence. Eve has no knowledge about these random frequency shifts, and should be quite difficult to pretend exactly like Bob. This provides the opportunity to detect the presence of Eve. We further develop an attack detection algorithm based on source enumeration

method. Both the asymptotic detection performance analysis and the numerical results are provided to verify the proposed studies. The results demonstrate that the proposed UFS scheme can achieve comparable detection performance as the existing superimposed random sequence based scheme [7], but with a substantially improved legitimate channel estimation performance.

Notations: Superscripts $(\cdot)^*$, $(\cdot)^T$ and $(\cdot)^H$ represent conjugate, transpose and Hermitian, respectively; $E[\cdot]$ denotes expectation; $\|\cdot\|$ denotes the Frobenius norm operator; $\mathbb{C}^{m \times n}$ defines the vector space of all $m \times n$ complex matrices; $\mathbf{j} = \sqrt{-1}$ is the imaginary unit; $\text{diag}(\mathbf{x})$ is a diagonal matrix with main diagonal of \mathbf{x} ; \mathbf{I}_N is the $N \times N$ identity matrix; $\mathbf{0}$ represents all-zero matrix with appropriate dimension.

II. SYSTEM MODEL

As illustrated in Fig. 1, we consider a transmission system with a legitimate transmitter Alice equipped with M antennas, a legitimate single-antenna user Bob, and an active eavesdropper Eve. We consider a TDD communication system, where the downlink channels and uplink channels are assumed to be reciprocal. The uplink reverse training phase is a typical way for Alice to obtain the channel information from Bob in order to apply beamforming in downlink data transmission. We consider the training pilot signals are repeatedly used and publicly known, which allows the smart eavesdropper Eve be able to transmit the same training signals to confound Alice.

The channels from Bob and Eve to Alice are respectively modeled as the following length- M vectors: $\mathbf{h} = [h(1), h(2), \dots, h(M)]^T$ and $\mathbf{g} = [g(1), g(2), \dots, g(M)]^T$. We assume each element of \mathbf{h} and \mathbf{g} follows i.i.d. complex Gaussian distribution with variance $1/M$, such that the total average channel gains from Bob and Eve at all receive antennas are normalized, i.e., $E[\|\mathbf{h}\|^2] = 1$ and $E[\|\mathbf{g}\|^2] = 1$.

Denote $\mathbf{s} = [s(1), s(2), \dots, s(N)]^T$ as the publicly known training sequence transmitted from Bob. Assume the symbols $s(n)$ are drawn from constant modulus constellations, i.e., $|s(n)| = 1$. Denote the transmit power of Bob and Eve by P_B and P_E , respectively. We define two events, \mathcal{H}_0 and \mathcal{H}_1 ; Namely, \mathcal{H}_0 : there exists no active eavesdropper who conducts pilot contamination attack; \mathcal{H}_1 : the active eavesdropper conducts pilot contamination attack trying to steal the information from the transmitter. Then, under perfect frequency synchronization, the received signal at Alice during the uplink training period can be expressed as the following $N \times M$ matrix:

$$\begin{aligned} \mathcal{H}_0: \quad \mathbf{Y} &= \sqrt{P_B} \mathbf{s} \mathbf{h}^T + \mathbf{N}, \\ \mathcal{H}_1: \quad \mathbf{Y} &= \sqrt{P_B} \mathbf{s} \mathbf{h}^T + \sqrt{P_E} \mathbf{s} \mathbf{g}^T + \mathbf{N} = \sqrt{P_B} \mathbf{s} \mathbf{h}_{\text{eq}}^T + \mathbf{N}, \end{aligned} \quad (1)$$

where $\mathbf{h}_{\text{eq}} = \mathbf{h}^T + \sqrt{\frac{P_E}{P_B}} \mathbf{g}^T$ and $\mathbf{N} \in \mathbb{C}^{N \times M}$ denotes the corresponding additive white Gaussian noise (AWGN) matrix. Assume each element of \mathbf{N} follows i.i.d. complex Gaussian distribution with variance σ_n^2 . It is clear that in the case of Eve's attack, Alice obtains a composite equivalent channel \mathbf{h}_{eq} instead of the expected \mathbf{h} . If Alice is unaware of attack and employs \mathbf{h}_{eq} as the legitimate channel information in

the downlink beamforming design, this not only degrades the signal reception quality at Bob but also leads to a significant signal leakage to Eve during the subsequent downlink data transmission.

III. PROPOSED TRAINING PHASE WITH UFS

From the comparison between (1) and (2), since Eve acts exactly in the same way as Bob, it is in fact quite difficult for Alice to distinguish whether Eve is presence or not. Motivated by the fact that frequency asynchronous nature would result in divergence between the transmitted signals from Bob and Eve, and thus may facilitate the detection of pilot contamination attack, we propose a new UFS scheme in this section to detect the pilot contamination attack.

Without loss of generality, we assume the length- N training sequence block can be divided into K equal-length segments, each with Q symbols, i.e., $N = K \times Q$. We can then split the whole training sequence block \mathbf{s} into

$$\mathbf{s} = [\mathbf{s}_1^T, \mathbf{s}_2^T, \dots, \mathbf{s}_K^T]^T, \quad (3)$$

where $\mathbf{s}_k = [s(1+(k-1)Q), s(2+(k-1)Q), \dots, s(kQ)]^T \in \mathbb{C}^{Q \times 1}$ denotes the pilot symbols in the k th segment. In the UFS scheme, Bob sends the pilot signals deliberately with some random CFO-like phase shifts. Specifically, let Bob independently select K artificial CFOs for each training segment, namely $\Delta f_{B,k}$, $k = 1, 2, \dots, K$. The normalized CFO of Bob in the k th segment can be expressed as $\phi_{B,k} = \Delta f_{B,k} T_s$, where T_s denotes the symbol rate interval. Thus, $2\pi\phi_{B,k}$ in fact represents the deliberately introduced phase shift of Bob over the consecutive pilot symbols in the k th training segment. On the other side, since Eve has no knowledge about the random artificial CFOs of Bob, she can also randomly select one trial CFO for each segment, denoted by $\Delta f_{E,k}$, $k = 1, 2, \dots, K$. Correspondingly, the normalized CFO of Eve in the k th training segment can be expressed as $\phi_{E,k} = \Delta f_{E,k} T_s$.

Let $\mathbf{E}(\phi) = \text{diag}(1, e^{j2\pi\phi}, \dots, e^{j2\pi\phi(N-1)})$ stand for the diagonal matrix representing the phase shift introduced by the CFO ϕ . The equivalent transmitted pilot symbols from Bob and Eve in the k th segment can be expressed as $\mathbf{E}(\phi_{B,k})\mathbf{s}_k$ and $\mathbf{E}(\phi_{E,k})\mathbf{s}_k$, respectively. Then, the received signals at Alice in the k th segment can be expressed as the following $Q \times M$ matrix:

$$\begin{aligned} \mathcal{H}_0: \quad \mathbf{Y}_k &= \sqrt{P_B} \mathbf{E}(\phi_{B,k}) \mathbf{s}_k \mathbf{h}^T + \mathbf{N}_k, \\ \mathcal{H}_1: \quad \mathbf{Y}_k &= \sqrt{P_B} \mathbf{E}(\phi_{B,k}) \mathbf{s}_k \mathbf{h}^T + \sqrt{P_E} \mathbf{E}(\phi_{E,k}) \mathbf{s}_k \mathbf{g}^T + \mathbf{N}_k, \end{aligned}$$

where $\mathbf{N}_k \in \mathbb{C}^{Q \times M}$ denotes the corresponding AWGN matrix, and each element of \mathbf{N}_k is i.i.d. complex Gaussian variable with variance σ_n^2 .

The attack detection algorithms at Alice based on the received signals \mathbf{Y}_k , $k = 1, 2, \dots, K$, will be developed in the following sections. Next, we first consider the CFO and channel estimation issue without Eve's attack. Specifically, when Eve is absent, the maximum-likelihood (ML) single-user CFO estimation and channel estimation at Alice can be

performed as follows:

$$\{\hat{\phi}_{B,k}, \hat{\mathbf{h}}\} = \arg \min_{\tilde{\phi}_{B,k}, \tilde{\mathbf{h}}} \sum_{k=1}^K \left\| \mathbf{Y}_k - \mathbf{E}(\tilde{\phi}_{B,k}) \mathbf{s}_k \tilde{\mathbf{h}}^T \right\|^2, \quad (4)$$

where $\tilde{\phi}_{B,k}$ and $\tilde{\mathbf{h}}$ stand for the trial CFO and channel for Bob, respectively. The CFO estimation solution of (4) can be expressed as

$$\hat{\phi}_{B,k} = \arg \max_{\tilde{\phi}} \left\| \mathbf{s}^H \mathbf{E}(\tilde{\phi})^H \mathbf{Y}_k \right\|^2, \quad (5)$$

which targets at maximizing the correlation between the pilot and the received signal after CFO compensation of a trial CFO $\tilde{\phi}$. The channel estimation solution can be then given by

$$\hat{\mathbf{h}}^T = \frac{1}{N} \sum_{k=1}^K \mathbf{s}^H \mathbf{E}(\hat{\phi}_{B,k})^H \mathbf{Y}_k. \quad (6)$$

Regarding the CFO and legitimate channel estimation performance of UFS scheme, we obtain the following *Lemma*:

Lemma 1: In the proposed UFS scheme, the CFO and channel estimation mean square error (MSE) under the high signal-to-noise ratio (SNR) condition in the absence of Eve's attack can be expressed as:

$$\text{MSE}(\hat{\phi}_{B,k}) = \frac{3\sigma_n^2}{2\pi^2 Q(Q^2 - 1) \|\mathbf{h}\|^2}, \quad (7)$$

$$\text{MSE}(\hat{\mathbf{h}}) = \frac{\sigma_n^2}{N} \left(\frac{3}{8\pi^2} \frac{Q-1}{Q+1} + M \right). \quad (8)$$

The detailed proof is omitted due to the space limitation. The following observations can be made from *Lemma 1*: First, as expected, the CFO estimation performance highly depends on the length of each training segment. This says that for better CFO estimation performance, a single training segment is preferred, that is, $K = 1$ and $Q = N$. However, this may not be a good choice for purpose of attack detection, which will be discussed in the following sections. Nevertheless, we see that the channel estimation performance, which is the main concerned issue in our work, is basically irrelevant to the segment length. In other words, the legitimate channel estimation performance is insensitive to the number of segments.

Second, the corresponding MSE performance without artificial frequency shifts in the conventional frequency synchronous channel estimation can be obtained as $M\sigma_n^2/N$. As compared to this conventional benchmark, the relative increased MSE in channel estimation of our UFS scheme can be expressed as $\frac{1}{M} \frac{3}{8\pi^2} \frac{Q-1}{Q+1} < \frac{1}{25M}$. The above discussions indicate that the multiple artificial frequency shifts in our UFS scheme introduce only negligible performance degradation in legitimate channel estimation, especially with more receive antennas at Alice. This differs from the existing superimposed random sequence based scheme [7] which suffers from a lot performance degradation in terms of the legitimate channel estimation.

IV. PROPOSED UFS-MDL DETECTION ALGORITHM

In this section, we develop a source enumeration based algorithm, referred to as 'UFS-MDL', to detect the presence of attack at Alice based on the received signals \mathbf{Y}_k ,

$k = 1, 2, \dots, K$. The corresponding asymptotic detection performance analysis is also provided.

A. Proposed Detection Scheme

Owing to the uncoordinated frequency shifts, our UFS training scheme introduces the divergence between the equivalent transmitted pilot signals between Bob and Eve. Hence, for the case $M \geq 3$, the minimum description length (MDL) algorithm [9] can be employed by Alice to detection the presence of Eve.

Specifically, the autocorrelation matrix for the k th training segment can be expressed as

$$\mathbf{R}_k = \frac{1}{Q} \mathbf{E} \left[\mathbf{Y}_k^T \mathbf{Y}_k^* \right]. \quad (9)$$

In the absence of attack, there holds

$$\mathcal{H}_0: \mathbf{R}_k = P_B \mathbf{h} \mathbf{h}^H + \sigma_n^2 \mathbf{I}_M, \quad (10)$$

which implies the dimension of signal subspace of \mathbf{R}_k is only one.

Let $\Delta\phi_k = \phi_{B,k} - \phi_{E,k}$ represent the CFO between Bob and Eve in the k th training segment. In the presence of Eve's attack, we have

$$\begin{aligned} \mathcal{H}_1: \mathbf{R}_k = & [\mathbf{h}, \mathbf{g}] \underbrace{\begin{bmatrix} \frac{P_B}{\sqrt{P_B P_E} \rho_k^*} & \frac{\sqrt{P_B P_E} \rho_k}{P_E} \end{bmatrix}}_{\mathbf{P}_k} [\mathbf{h}, \mathbf{g}]^H \\ & + \sigma_n^2 \mathbf{I}_M. \end{aligned} \quad (11)$$

Here, $\mathbf{P}_k \in \mathbb{C}^{2 \times 2}$ represents the correlation of the equivalent transmitted pilot signals between Bob and Eve, where

$$\rho_k = \frac{1 - e^{j2\pi Q \Delta\phi_k}}{Q(1 - e^{j2\pi \Delta\phi_k})}. \quad (12)$$

Theoretically, when $\Delta\phi_k \neq 0$, we have

$$\det(\mathbf{P}_k) = P_B P_E (1 - |\rho_k|^2) > 0, \quad (13)$$

saying \mathbf{P}_k is nonsingular in this case. The dimension of signal subspace of \mathbf{R}_k is two when $\Delta\phi_k \neq 0$.

Following the above discussions under \mathcal{H}_0 and \mathcal{H}_1 , the MDL criterion [9] can be employed to determine the dimensional of signal subspace. Specifically, denote the eigenvalues of $\hat{\mathbf{R}}_k = \frac{1}{Q} \mathbf{Y}_k^T \mathbf{Y}_k^*$ in descending order by $\lambda_k(i)$, $i = 1, 2, \dots, M$. The MDL estimation of signal subspace dimension for $\hat{\mathbf{R}}_k$ can be given by

$$\hat{d}_k = \arg \min_{1 \leq d \leq M-1} \text{MDL}_k(d), \quad (14)$$

where

$$\begin{aligned} \text{MDL}_k(d) = & - \sum_{i=d+1}^M \log(\lambda_k(i)) + (M-d) \log \left(\frac{\sum_{i=d+1}^M \lambda_k(i)}{M-d} \right) \\ & + \frac{d(2M-d) \log(Q)}{2Q}. \end{aligned} \quad (15)$$

When the signal subspace dimension of at least one training segment is above one, i.e., $\max_k \hat{d}_k > 1$, we declare the presence of Eve's attack. Otherwise, we consider the Eve's attack is absence.

B. Asymptotic Performance Analysis

In the subsection, we provide asymptotic performance analysis for the proposed UFS-MDL detection algorithm. We consider the high SNR condition. Moreover, both the training sequence length and the receive antenna number at Alice are assumed to be very large, i.e., $N \gg 1$ and $M \gg 1$. Note that there is an increasing interest from both academy and industry to equip base station with a large scale antenna array [12], [13], such a system can provide a remarkable increase in both reliability and spectral efficiency. We focus on the asymptotic false negative (miss detection) probability, which is defined as the probability when miss of detection happens. The following Lemma can be obtained:

Lemma 2: Assume the random normalized CFOs of Bob and Eve follow uniform distribution from $-\phi_{\max}$ to ϕ_{\max} with $|\phi_{\max}| < 0.5$. Denote $P_{th} = M(\sqrt[Q]{Q} - 1)\sigma_n^2$. When the minimum power of Bob and Eve is larger than P_{th} , i.e., $\min(P_B, P_E) > P_{th}$, the asymptotic miss detection probability of the UFS-MDL detection algorithm can be approximately upper bounded by

$$\mathcal{P}_{MDL} = \left(\frac{2}{\pi Q \phi_{\max}} \arccos \sqrt{\left(1 - \frac{P_{th}}{P_B}\right) \left(1 - \frac{P_{th}}{P_E}\right)} \right)^K. \quad (16)$$

Otherwise, when $\min(P_B, P_E) \leq P_{th}$, the miss detection probability of UFS-MDL approximately equal one, i.e., $\mathcal{P}_{MDL} \lesssim 1$. The detailed proof is omitted due to the space limitation. The following observations can be made from Lemma 2: 1) As expected, the miss detection probability of UFS-MDL can be reduced by increasing the range of random artificial CFOs. The asymptotic miss detection probability is also relevant to the noise power and the number of receive antennas. There exists a cliff-like jump of miss detection probability when the minimum power between Bob and Eve becomes less than P_{th} . 2) We see that the detection performance of UFS-MDL can always benefit from the increased attack power from Eve. Interestingly, the detection performance will asymptotically touch a lower bound when attack power P_E becomes very large. Specifically, when $P_E \gg P_B$, according to (16), the asymptotic lower bound of UFS-MDL can be obtained as

$$\mathcal{P}_{MDL} \gtrsim \left(\frac{2}{\pi Q \phi_{\max}} \arccos \sqrt{\left(1 - \frac{P_{th}}{P_B}\right)} \right)^K. \quad (17)$$

It is observed that this lower bound can be simply reduced by a larger transmit power at Bob. 3) The equation (16) also demonstrates the benefit from the multiple frequency shifts in UFS-MDL.

V. SIMULATIONS

In this section, we provide numerical results to evaluate the performance of the proposed scheme. Assume the pilot symbols are randomly drawn from QPSK constellation. Unless otherwise specified, the pilot length is taken as $N = 64$ and let normalized artificial CFOs of Bob and Eve in each training

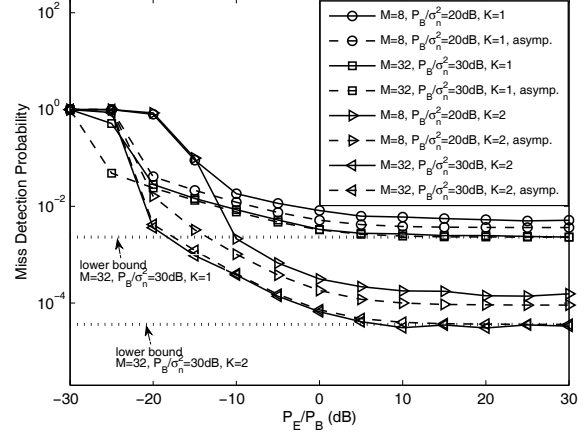


Fig. 2. Miss detection probability of the proposed UFS-MDL algorithm with different relative power between Bob and Eve. The corresponding asymptotic analytical performance is included as the dashed curves, while the asymptotic lower bound in (17) is plotted as the dotted curves.

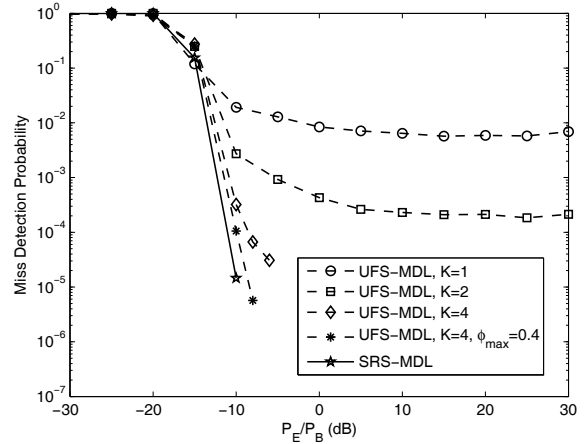


Fig. 3. Detection performance comparison between the SRS-MDL scheme [7] and the proposed UFS scheme ($M = 16$, $P_B/\sigma_n^2 = 20$ dB).

segment follow uniform distribution from -0.2 to 0.2 , i.e., $\phi_{\max} = 0.2$.

In Fig. 2, we show miss detection probability of our UFS-MDL algorithm as a function of the relative power between Bob and Eve (P_B/P_E) under different SNR condition P_B/σ_n^2 . The following observations can be made. First, as expected, the performance of UFS-MDL can be improved with stronger signal power from Eve. Second, we see that the simulation results closely match the corresponding asymptotic results, which verifies the correctness of the asymptotic analysis. Especially, when Eve has much stronger power than Bob, we can observe that the detection performance converges to the analytical lower bound given by (17).

The detection performance of UFS-MDL with different K is plotted in Fig. 3. We also include the performance of the superimposed random sequence based MDL scheme [7], labelled as ‘SRS-MDL’. The results show that when Eve has smaller or similar power as Bob, the proposed scheme can achieve comparable detection performance as SRS-MDL with a relative large K and a larger maximum artificial CFO ϕ_{\max} .

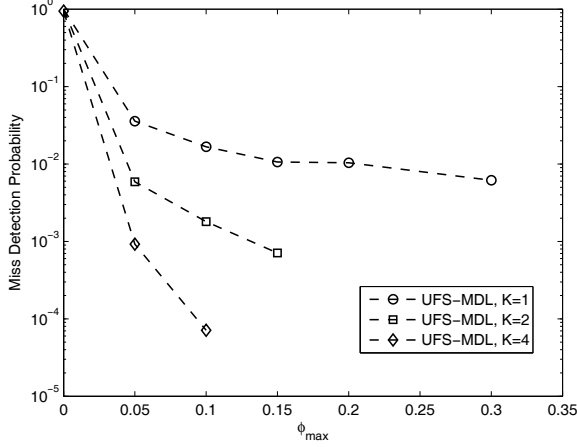


Fig. 4. Detection performance of the proposed UFS scheme with different maximum artificial CFOs ($M = 16$, $P_B/\sigma_n^2 = 20\text{dB}$ and $P_B = P_E$).

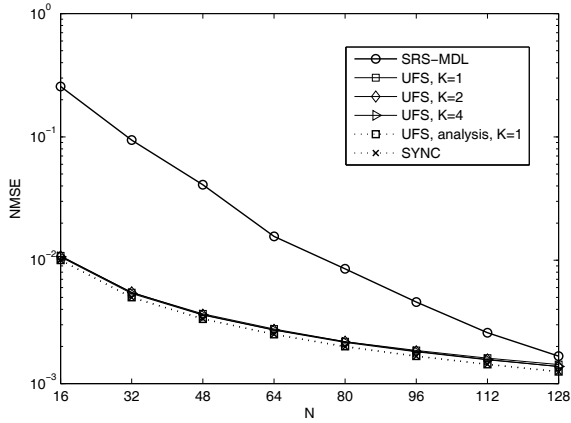


Fig. 5. Channel estimation performance comparison between the SRS-MDL scheme [7] and the proposed UFS scheme.

However, SRS-MDL behaves better in the region with much stronger attack power. Note that the performance of UFS-MDL approaches a lower bound as the attack power increases. Nevertheless, as the random sequences are superimposed in the pilot signal in SRS-MDL, our UFS scheme could substantially outperform SRS-MDL in terms of channel estimation, which will be demonstrated below.

In Fig. 4, we increase the maximum artificial CFO ϕ_{\max} from 0 to 0.3 and demonstrate the detection performance evolution of our UFS scheme. As expected, we see that the detection performance of our proposed UFS scheme can be improved by increasing the maximum artificial CFOs. The results also clearly indicate the benefit of multiple segments. It is seen that, in the case of more segments, i.e., a larger K , more random artificial CFOs are introduced and the miss detection probability could decline more quickly as the maximum CFO increases.

In the last, we plot the channel estimation performance comparison between SRS-MDL and our UFS scheme in Fig. 5. The MSE of channel estimation is adopted as the figure of merit.

We assume absence of Eve in this example. The iterative channel estimation method is employed in SRS-MDL as described in [7]. It is seen that the channel estimation performance of both SRS-MDL and our scheme improves with increasing the pilot signal length. Moreover, our scheme show no much changes with different K . Note that SRS-MDL superimposes the self-contamination random sequences in the pilot signal, inevitably degrading the performance of legitimate channel estimation. In comparison, our scheme could outperform SRS-MDL especially with a shorter pilot sequence. On the other side, we include the corresponding analytical results from (8) with $K = 1$ in this figure, plotted as the dotted curve. The conventional channel estimation performance with frequency synchronization is also included, labelled as ‘SYNC’. It is observed that the simulation results of our scheme closely approach the analytical curve and the SYNC benchmark. This coincides with our previous observation that the proposed UFS scheme basically does not sacrifice the legitimate channel estimation performance for attack detection.

VI. CONCLUSIONS

In this paper, we proposed a new UFS scheme for detection of pilot contamination attack. The proposed scheme deliberately introduces multiple random frequency shifts in the transmitted pilot signal from the legitimate user Bob. A detection algorithms were designed for Alice to detect the presence of attack. We also provided both the asymptotic performance analysis and numerical results to verify the proposed studies.

REFERENCES

- [1] X. Zhou, B. Maham and A. Hjørungnes, “Pilot contamination for active eavesdropping,” *IEEE Trans. Wireless Commun.*, vol. 11, pp. 903–907, Mar. 2012.
- [2] D. Kapetanovic, G. Zheng, K.-K. Wong, and B. Ottersten, “Detection of pilot contamination attack using random training and massive MIMO,” in *Proc. IEEE PIMRC*, pp. 13–18, London, UK, Sept. 2013.
- [3] D. Kapetanovic, A. Al-Nahari, A. Stojanovic, and F. Rusek, “Detection of active eavesdroppers in Massive MIMO,” in *Proc. IEEE PIMRC*, pp. 585–589, 2014.
- [4] J. Yang, S. Xie, X. Zhou, R. Yu, and Y. Zhang, “A semiblind two-way training method for discriminatory channel estimation in MIMO systems,” *IEEE Trans. Commun.*, vol. 62, no. 7, Jul. 2014.
- [5] J.-M. Kang, C. In, and H.-M. Kim, “Detection of pilot contamination attack for multi-antenna based secrecy systems,” in *Proc. IEEE VTC Spring*, May 2015.
- [6] Q. Xiong, Y.-C. Liang, K. H. Li, and Y. Gong, “An energy-ratio based approach for detecting pilot spoofing attack in multiple-antenna systems,” *IEEE Trans. Info. Forensics & Security*, vol. 10, pp. 932–940, May 2015.
- [7] J. K. Tugnait, “Self-contamination for detection of pilot contamination attack in multiple antenna systems,” *IEEE Wirelss Commun. Lett.*, vol. 4, no. 5, Oct. 2015.
- [8] J. K. Tugnait, “Detection of pilot contamination attack in T.D.D./S.D.M.A. systems,” in *Proc. IEEE ICASSP*, 2016.
- [9] M. Wax and T. Kailath, “Detection of signals by information theoretic criteria,” *IEEE Trans. Acoustics, Speech, Signal Proc.*, vol. 33, no. 2, pp. 387–392, Apr. 1985.
- [10] W. Zhang and Q. Yin, “Blind maximum likelihood carrier frequency offset estimation for OFDM with multi-antenna receiver,” *IEEE Trans. Signal Process.*, vol. 61, no. 9, May 2013.
- [11] W. Zhang and F. Gao, “Blind frequency synchronization for multiuser OFDM uplink with large number of receive antennas,” *IEEE Trans. Signal Process.*, vol. 64, no. 9, pp. 2255–2268, May 2016.
- [12] H. Xie, F. Gao, S. Zhang, and S. Jin, “A unified transmission strategy for TDD/FDD massive MIMO systems with spatial basis expansion model,” to appear in *IEEE Trans. Veh. Technol.*, 2016.

- [13] H. Xie, F. Gao, and S. Jin, An overview of low-rank channel estimation for massive MIMO systems, *IEEE Access*, vol. 4, Nov. 2016.